

Raspodijeljene glavne knjige i kriptovalute

Ekosustav kriptovaluta

Ante Đerek, Zvonko Konstanjčar

20. siječnja 2022.

Odabrani izazovi u krypto sustavima

- Anonimnost
 - Želimo razinu privatnosti kao kod klasičnih bankarskih sustava (ili veću)
- Skalabilnost
 - Mikroplaćanja ne funkcioniraju
 - Lightning network (L2 rješenja)
- Regulativa
 - Puno argumenata protiv
 - Tržišta ne rezultiraju uvijek ishodima koji su dobri za većinu sudionika tržišta (pogotovo u kratkom roku)

Decentralizirane financije

- Decentralizirane stabilne kriptovalute
- Decentralizirano kreditiranje
- Decentralizirane burze

Sadržaj

- Analiza stanja
- Tehnološka perspektiva
- Ekonomska i poslovna perspektiva
- Financijska perspektiva

Ukupna tržišna kapitalizacija



Izvor: coinmarketcap.com/charts/

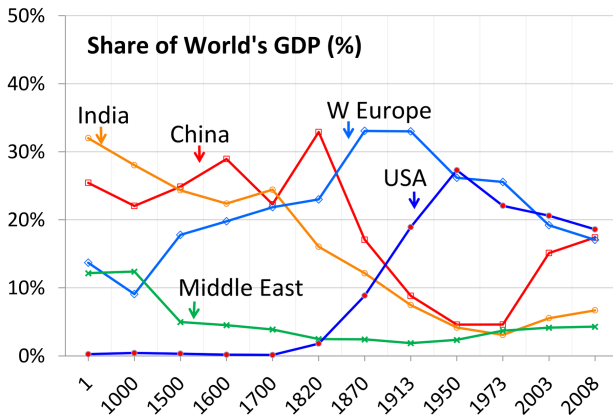
Zadatak

Koliko je ukupna vrijednost zlata?

Izvor: <http://money.visualcapitalist.com>

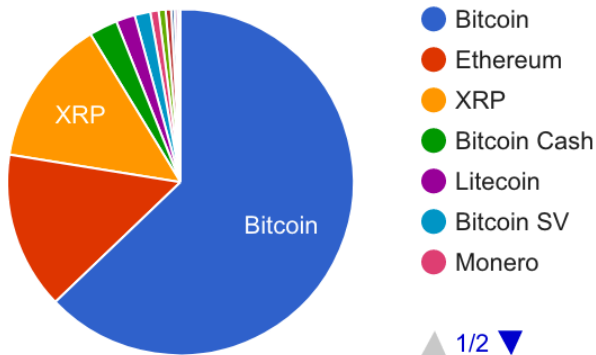
- Ukupno bogatstvo Bill Gatesa: 134 milijardi
- Ukupna vrijednost srebra: 1.34 bilijuna
- Ukupna vrijednost kripto tržišta: 2 bilijuna
- Ukupna tržišna kapitalizacija Applea: 2.7 bilijuna
- Ukupna vrijednost novčića i novčanica: 6.6 bilijuna
- Ukupna vrijednost zlata: 11.7 bilijuna
- Ukupna vrijednost tržišta dionica: 93.7 bilijuna
- Ukupna vrijednost novca (novčići, novčanice, razni računi, depoziti): 95.7 bilijuna
- Ukupna vrijednost globalnog duga: 253 bilijuna (322% globalnog BDP-a)
- Ukupna vrijednost nekretnina: 280 bilijuna
- Ukupna vrijednost tržišta derivativa: 11-558 bilijuna

Dinamika globalnog BDP-a










Izvor: By M Tracy Hunter - Own work, CC BY-SA 4.0,
<https://commons.wikimedia.org/w/index.php?curid=34088589>

Market Capitalization, \$USD



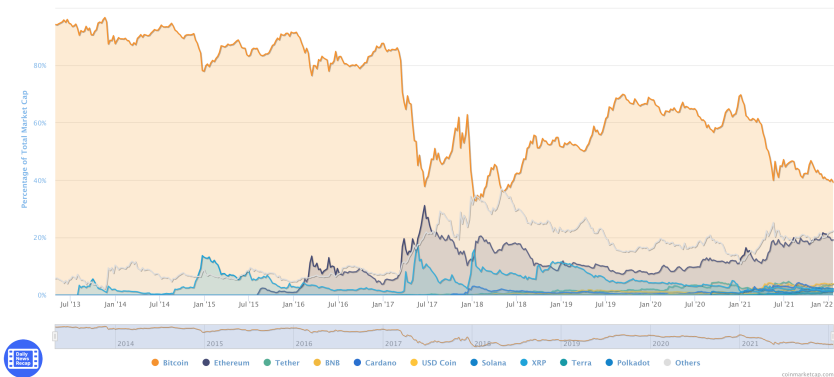
Izvor: bitinfocharts.com/cryptocurrency-charts.html

Ukupna tržišna kapitalizacija - vodeći altcoini

# ▼	Name	Price	24h %	7d %	Market Cap ⓘ
1	 Bitcoin BTC Buy	\$42,210.59	▲ 1.63%	▼ 2.86%	\$799,118,201,417
2	 Ethereum ETH Buy	\$3,131.59	▲ 0.19%	▼ 5.66%	\$373,382,985,461
3	 Tether USDT Buy	\$1.00	▲ 0.03%	▼ 0.02%	\$78,343,276,644
4	 BNB BNB Buy	\$466.62	▲ 1.06%	▼ 1.50%	\$77,003,407,545
5	 Cardano ADA	\$1.43	▼ 3.10%	▲ 14.15%	\$47,859,492,672
6	 USD Coin USDC	\$0.9994	▼ 0.08%	▼ 0.08%	\$45,813,688,788
7	 Solana SOL Buy	\$137.15	▲ 1.09%	▼ 4.20%	\$43,127,693,149

Izvor: coinmarketcap.com/

Ukupna tržišna kapitalizacija



Izvor: coinmarketcap.com/charts/

Osnivanje	Naziv	Konsenzus	Komentar
2009	Bitcoin	PoW	Digitalni novac/zlato
2015	Ethereum	PoW	Pametni ugovori, tokeni
2015	Tether	PoW	Cijena = 1 USD
2017	Binance Coin	varijanta PoS	Plaćanje usluga na Binance burzi
2017	Cardano	Ouroboros PoS	Pametni ugovori, tokeni
2018	USD Coin	PoW	Cijena = 1 USD
2019	Solana	PoS i "proof-of-history"	Pametni ugovori, tokeni

Prva generacija

- Fokus na digitalnom novcu, primjer Bitcoin
- Koriste kriptografske lance blokova

Druga generacija

- Fokus na pametnim ugovorima, primjer Ethereum
- Koriste kriptografske lance blokova

Treća generacija

- Fokus na mikroplaćanja
- Koriste usmjerene acikličke grafove (DAG)
- Primjer IOTA (tangle struktura podataka)
 - paralelna validacija: svaki član mreže koji želi izvršiti transakciju mora validirati dvije postojeće transakcije
 - nagrada za validaciju nisu novi tokeni (ima ih fiksna broj)
 - mreža postaje brža što je više ljudi koristi

Raspodijeljena glavna knjiga

Baza podataka koja je replicirana na mnoštvu čvorova u mreži.

- Svaki čvor održava svoju kopiju baze, podaci u svakom čvoru su identični
- Postoji mehanizam koji omogućuje čvorovima da sinkroniziraju promjene i održavaju identične kopije.

Kriptografski lanac blokova

Kriptografski lanac blokova je jednostruko povezana lista u kojoj svaki element (uz neke podatke) sadrži hash pokazivač na prethodni element.

Bitcoin mreža: jednostavna P2P mreža

- Nema posebnih čvorova niti posebne topologije
- Čvorovi se slobodno mogu pridružiti ili napustiti mrežu

Sudionici u mrežama

- *Pisac* - bilo koji čvor koji može upisivati u glavnu knjigu
 - u kriptografskim lancima blokova to su čvorovi koji sudjeluju u rastu lanca
 - prikupljaju transakcije i spremaju ih u blokove te dodaju blok u lanac blokova
 - mogu validirati zapise
- *Čitatelj* - bilo koji čvor u mreži koji ne sudjeluje u upisivanju u glavnu knjigu
 - bilo koji čvor koji ne sudjeluje u produljenju lanca blokova
 - sudjeluje u procesu kreiranja transakcija
 - može validirati transakcije
 - može čitati i analizirati lanac blokova

U ove kategorije ne uključujemo developere i regulatore.

S dozvolama vs bez dozvola (engl. premissioned vs premissionless)

- Bez dozvola
 - u bilo kojem trenutku bilo koji čvor može napustiti mrežu ili joj se može pridružiti kao pisac ili čitatelj
 - ne postoji centralni autoritet koji bi određivao tko što smije
- S dozvolom
 - postoji centralni autoritet koji odlučuje koji čvorovi se mogu pridružiti mreži i koji dodjeljuje čvorovima prava pisanja i čitanja

Javni vs privatni (engl. public vs private)

- Javni - bilo tko može čitati informacije iz lanca blokova
- Privatni - postoji centralni autoritet koji odlučuje tko može vidjeti koje informacije

Javna provjera

Bilo tko može provjeriti ispravnost stanja sustava

- Kod Bitcoina čvorovi provjeravaju ispravnost lanca blokova, ali može i bilo tko izvan
- Kod centraliziranih sustava promatrači često nemaju uvid u kompletno stanje sustava te moraju vjerovati centralnom autoritetu o ispravnosti stanja sustava

Transparentnost

Transparentnost podataka i pravila za ažuriranje stanja sustava je preduvjet za javnu provjeru

Privatnost

Lakše postići u centraliziranim sustavima, jer za njihovo funkcioniranje nije potrebna javna provjera

Raspodijeljene glavne knjige možemo realizirati kao

- Bez dozvole, javna glavna knjiga (Bitcoin, Ethereum, itd.)
- S dozvolom, javna glavna knjiga (Ripple, itd.)
- S dozvolom, privatna glavna knjiga (Hyperledger Fabric, R3 Corda, itd.)
- Tradicionalna baza podataka

Mehanizmi za kontrolu distribuiranih glavnih knjiga

- Proof of work (PoW)
- Proof of Stake (PoS)
- Treća strana radi verifikaciju, itd.

Kako odabrati glavnu knjigu?

- Informacije
 - postoji li potreba za spremanjem informacija (što znamo o tim informacijama, u kakvim su formatima)?
 - postoji li želja/potreba za objavljivanjem transakcija javno ili ih smiju vidjeti samo određeni korisnici?
- Zajedničko upisivanje
 - postoji li potreba za zajedničkim upisivanjem?
 - tko može pisati u knjigu (znaju li se svi pisci, ima li ih fiksni broj, imaju li iste interese, može li im se vjerovati)?
- Povjerenje
 - vjeruju li si *pisci* međusobno?
 - postoji li treća strana (ili više njih) kojoj svi vjeruju (je li ona stalno *online*, radi li ona dobro svoj posao)?
 - treba li itko imati prave informacije o *piscima* (što ako lažu, trebaju li potpisati ugovore za pristupanje mreži)?

Kada trebamo kriptografske lance blokova?

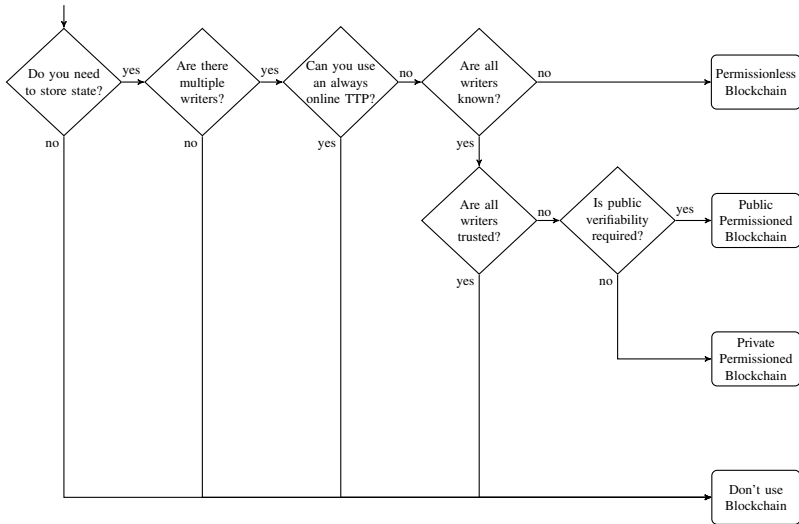
Osnovna ideja

S dozvolom ili bez dozvole kriptografske lance blokova ima smisla koristiti jedino kada više entiteta koji si međusobno ne vjeruju žele interagirati i zajedno mijenjati stanje sustava, a ne mogu se dogovoriti oko online treće strane kojoj svi vjeruju (TTP).

Kompromis između decentralizacije i propusnosti

Što više ima entiteta koji si međusobno ne vjeruju to manje ažuriranja stanja po entitetu sustav može napraviti u jedinici vremena.

Kada trebamo kriptografske lance blokova?



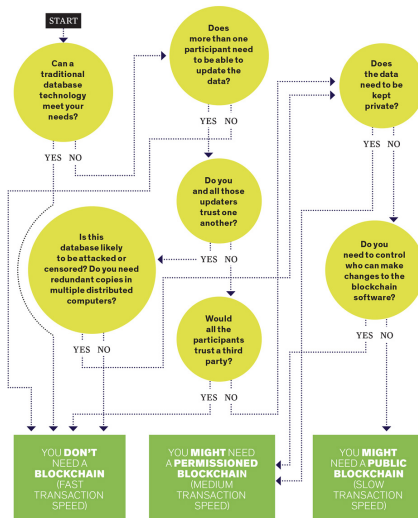
Izvor: K. Wüst and A. Gervais, "Do you Need a Blockchain?," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 2018, pp. 45-54. doi: 10.1109/CVCBT.2018.00011

Kada trebamo kriptografske lance blokova?

	Permissionless Blockchain	Permissioned Blockchain	Central Database
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	Mainly PoW, some PoS	BFT protocols (e.g. PBFT [5])	None
Centrally managed	No	Yes	Yes

Izvor: K. Wüst and A. Gervais, "Do you Need a Blockchain?," 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 2018, pp. 45-54. doi: 10.1109/CVCBT.2018.00011

Kada trebamo kriptografske lance blokova?



lzvor: ieeexplore.ieee.org/computing/networks/do-you-need-a-blockchain

Kada trebamo javne, bez dozvole lance blokova?

Načelno: U poslovima u kojima trebamo/želimo ostvariti prijenos imovine bez posredovanja treće strane.

Eliminacijom "treće strane"

- Imamo veću sigurnost
- Imamo jeftiniju uslugu?

Pokazalo se da je teško realizirati takav sustav, a da je različit od izvornih kriptovaluta (npr. Bitcoin).

Problemi (ako eliminiramo odgovarajuće izvorne kriptovalute)

- Ulaz i izlaz informacija u sustav
- Osiguravanje nepromjenjivosti

Potrebna je "treća strana" kojoj svi vjeruju

- Ona osigurava nepromjenjivost
- Ona definira komunikaciju sa sustavom

Postoje slučajevi u kojima su kriptografski lanci blokova s dozvolom pravo rješenje, ali za veći broj problema su centralizirani sustavi efikasniji i pouzdaniji.

Stvoren je ogromni interes za lance blokova

- I velike i male kompanije razmatraju poslovne scenarije
- Očekivanja su velika
 - nova tehnologija će sniziti troškove poslovanja
 - nova tehnologija otvara nove poslovne prilike
- Transakcije će biti
 - brže
 - sigurnije
 - transparentnije
 - decentralizirane

Trenutno tehnologiju iza **lanca blokova** većina ne razumije dovoljno.

Ne postoji konsenzus oko **prednosti** i **nedostataka** koje tehnologija donosi.

Većina prednosti koja se pripisuje tehnologiji ulančanih blokova ne dolazi iz te tehnologije.

Ključni koncepti

- Pametni ugovori
- Enkripcija
- Raspodijeljena glavna knjiga

Koncepti se mogu implementirati zajedno, ali ne nužno.

Većina prednosti dolazi iz pametnih ugovora i enkripcije.

U širem smislu pametni ugovori su računalni programi u kojima su implementirani uvjeti ugovora između stranaka.

Primjeri

- Trajni nalog - automatsko plaćanje obaveza
- Ograničeni nalozi na burzama

Pametni ugovori se mogu kreirati u okviru raznih postojećih centraliziranih sustava.

Znatne uštede su moguće korištenjem enkripcije u raznim domenama poslovanja, ali to također nije nužno vezano uz tehnologije ulančanih blokova.

Trenutno - samo ograničena primjena

- Bitcoin kao platežno sredstvo - za ograničen skup dobara i usluga
- Teško se može nositi s trenutnim sustavima plaćanja

Što se može decentralizirati?

- Pametno vlasništvo - npr. pametni auto, bicikl
- Digitalne investicije - npr. fiat valute, dionice, druga imovina
- Kompleksni ugovori - npr. financijski derivati
- Tržišta i aukcije - npr. tržište rabljenih bicikala, tržišta dionica
- Burze i plaćanja - npr. BTC - USD (TTD, Ripple)

Kada ima smisla decentralizirati?

- Problemi kod pametnog vlasništva
 - tradicionalne institucije donose dvije stvari: (a) osiguravaju vlasništvo i (b) osiguravaju sigurnu razmjenu
 - što kada se dogodi problem?
- Mora postojati ekonomsko opravdanje - npr. neefikasna regulativa, značajan nedostatak povjerenja, itd.

Financijska perspektiva - klasifikacija investicija

Imovina (engl. asset)

Samim držanjem vlasniku generira tokove novca. Primjeri su poslovi, nekretnine, obveznice, dionice itd.

Roba (engl. commodity)

Predstavljaju ulaz u proces koji ima uporabnu vrijednost. Primjeri su plin, nafta, kukuruz, itd.

Valuta (engl. currency)

Primarne funkcije su: (a) obračunska jedinica, (b) sredstvo razmjene te (c) pohrana vrijednosti.

Kolekcionarski predmet (engl. collectible)

Ne generira tokove novca i ne služi kao sredstvo razmjene, ali može imati estetsku ili emocionalnu vrijednost. Primjeri su umjetnine, zbirke novčića, itd.

Investiranje i trgovanje u užem smislu

Na cijenu investicije utječe

- Intrinzična "prava" vrijednost investicije (pogotovo dugoročno)
- Odnos ponude i potražnje

Investiranje - fokus na apsolutnim iznosima (intrinzičnoj vrijednosti)

Cilj je odrediti intrinzičnu vrijednost investicije te se investira ako je trenutna cijena ispod intrinzične vrijednosti.

Trgovanje - fokus na relativnim odnosima (cijeni)

Cilj je predvidjeti statističke karakteristike cijena u budućnosti te trgovati sukladno predikcijama.

Nesigurnost procjene intrinzične vrijednosti

Pouzdanost procjene intrinzične vrijednosti se dosta razlikuje od investicije do investicije.

Investiranje i trgovanje u užem smislu

Investicije	Investiranje	Trgovanje
Imovine	Na temelju očekivanih tokova novca i rizika	Povijesne cijene i drugi dostupni podatci
Robe	Na temelju ponude i potražnje za finalnim proizvodima uz nesiguran vremenski raskorak (teško)	Povijesne cijene i drugi dostupni podatci
Valute	Vrlo teško	Povijesne cijene i drugi dostupni podatci, uz to da šire prihvaćanje valute kao sredstva razmjene i stabilnija kupovna moć (manja inflacija) implicira više cijene
Kol. predmet	Vrlo teško	Na temelju procjene atraktivnosti i nestašice

Što je Bitcoin?

Nije imovina

Ne generira tokove novca vlasniku koji ga posjeduje, do trenutka prodaje.

Nije roba

Nije sirovina potrebna za izgradnju nečeg korisnog. Kod Ethereum, gas se koristi kao sirovina za pametne ugovore.

Valuta ili kolekcionarski predmet?

Više ljudi percipira Bitcoin kao valutu.

Zadatak

Kako klasificiramo zlato?

Utjecaj na cijenu

Ako je valuta onda na cijenu Bitcoina utječe:

- Koliko ljudi ga koristi kao sredstvo plaćanja
- Koliko je stabilna kupovna moć - koliko dobro čuva vrijednost

Trenutno ne pokazuje karakteristike dobre valute

- Kao sredstvo razmjene koristi ga mali broj ljudi
- Previše je volatilan kao sredstvo čuvanja vrijednosti

Zašto se ne koristi više u transakcijama?

Inercija

Fiat valute imaju dugu povijest i većina ljudi ih "razumije" te ima jasan stav o njima.

Volatilnost cijena

- Većinu kriptovaluta karakteriziraju velike fluktuacije u cijenama, što nije nužno loše kod imovine, ali kod valuta je
- Prodavač koji svoje proizvode (ili usluge) naplaćuje u Bitcoinima treba konstantno korigirati cijene kako bi se održala stalna vrijednost u kratkim vremenskim razmacima.

Konkurentne kriptovalute

- Kriptotržište je u razvoju i svakodnevno se javljaju nove valute koje bi mogle postati vodeće digitalne valute
- Kako će tržište sazrijevati tako će postati jasno koje valute treba koristiti, trenutno postoji strah da se ne investira u krive

Budući scenariji za Bitcoin kao valutu

Pozitivni: globalna digitalna valuta

U njemu BTC postaje globalna digitalna valuta koja se koristi diljem svijeta kao sredstvo plaćanja. U tom scenariju postaje usporediva s fiat valutama po karakteristikama i predviđa joj se visoka cijena u odnosu na druge fiat valute.

Neutralni: zlato za milenijalce

U njemu BTC postaje sredstvo plaćanja za one koji ne vjeruju centralnim bankama, vladama i fiat valutama. U tom scenariju postaje kao zlato u prošlim vremenima, utočište za one koji izgube vjeru u institucije. Tada se očekuje rast u periodima krize, a pad u periodima rasta gospodarstva.

Negativni: tulipani 21 stoljeća

U njemu BTC raste samo zato što kupci vjeruju da će u budućnosti još više rasti, ali nakon što se kupci prebace na nešto drugo slijedi vrtoglav pad.

Gotovo sigurno će biti vrednovan kao valuta

U dugom roku cijena će ovisiti o tome koliko dobro će ispunjavati funkcije valute. Ako će biti široko prihvaćen kao sredstvo razmjene te će biti dovoljno stabilan da može služiti kao sredstvo pohrane vrijednosti tada će s pravom imati visoku cijenu.

Trenutno nije prepoznat kao sredstvo plaćanja, nego kao špekulativna investicija

Na žalost, ono zbog čega su kriptovalute zanimljive traderima (visoka volatilnost), čini ih neprihvatljivim ljudima koji bi ih koristili kao platežno sredstvo.

Disruptivni karakter

- Očekuje se veliki utjecaj na razne industrije, ne samo financijsku
- Postoji šansa da se to ne realizira prema trenutnim vizijama
- I etablirana i nova poduzeća pomno prate i analiziraju tehnologiju
 - shvaćaju vrijednost enkripcijskih alata i pametnih ugovora

Rizik: svijet iza kriptografskih lanaca blokova mogao bi biti i **svijet bez kriptografskih lanaca blokova**.

Važno uočiti: Izvan Bitcoina (i sličnih kriptovaluta) **ne postoji** tehnologija koja omogućuje realizaciju **bez dozvola raspodijeljene glavne knjige s osiguranom nepromjenjivošću bez treće strane**.

Veliki problem danas: **nedostatak povjerenja** (glavna primjena).